



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/789,975

02/27/2004

Jean-Marie Gatto

CYBS5858

9438

22430

7590

10/11/2006

YOUNG LAW FIRM, P.C.

ALAN W. YOUNG

4370 ALPINE ROAD

SUITE 106

PORTOLA VALLEY, CA 94028

EXAMINER

SON, LINH L D

ART UNIT

PAPER NUMBER

2135

DATE MAILED: 10/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No.	Applicant(s)	
	10/789,975	GATTO ET AL.	
	Examiner	Art Unit	
	Linh LD Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 26 September 2006.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-79 and 81-97 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-79, and 81-97 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.

- Chandray B. M.*  
**AMZ135**
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_.

### **DETAILED ACTION**

1. **This Office Action is responding to the RCE received on 09/26/06.**
2. **Claims 1-79, and 81-97 are pending.**

#### ***Claim Rejections - 35 USC § 102***

3. **The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:**

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. **Claims 20-23, 71-79, and 81, and 94-97 are rejected under 35 U.S.C. 102(e) as being anticipated by Rabin et al, US Patent No. 6697948B1, hereinafter "Rabin".**

5. **As per claim 20:**

Rabin discloses "A method for a network connected gaming system to enable only authorized software components of constituent computers of the gaming system to execute, comprising the steps of:

Art Unit: 2135

configuring a separate for each authorized software component in each of the constituent computers of the gaming system; and enforcing the software restriction policy for each authorized software component such that the each authorized software component in each of the constituent computers of the gaming system must be authorized to run by its associated separate software restriction policy." in (Col 26 lines 50-60, Col 27 lines 30-44, Col 28 lines 5-15, Col 28, Table 1, line 30 to Col 30 line 20, and Col 52 line 60 to Col 53 line 25).

*Rabin creates a PKI certificate specifically with unique software call-up policy for each unique Hardware ID. It is clearly that the gaming system must be authorized to run by its associated separate software restriction policy. (Col 28 lines 30-65).*

**6. As per claim 21:**

Rabin discloses "A method according to claim 20, wherein the authorized software components are mandated by a regulatory body" in (Col 26 lines 50-60, Col 27 lines 30-44, Col 28 lines 5-15, Col 28, Table 1, line 30 to Col 30 line 20, and Col 52 line 60 to Col 53 line 25).

**7. As per claim 22:**

Rabin discloses "A method for a network connected gaming system to enable only authorized software components of constituent computers of the gaming system to execute, comprising the steps of:

configuring a separate and unique certificate software restriction policy for each authorized executable software component of each of the constituent computers of the

Art Unit: 2135

gaming system such that the each authorized executable software component in each of the constituent computers of the gaming system must be authorized to run by its associated separate software restriction policy" in (Col 26 lines 50-60, Col 27 lines 30-44, Col 28 lines 5-15, Col 28, Table 1, line 30 to Col 30 line 20, and Col 52 line 60 to Col 53 line 25);

“configuring a path software restriction policy to prevent unauthorized software components from executing;

configuring a path software restriction policy to prevent non-explicitly authorized software components from executing;

enforcing the certificate software restriction policy configured for each of the authorized executable software components of each of the constituent computers of the gaming system, and enforcing the path software restriction policies” in (Col 47 line 56 to Col 48 line 33, and Col 52 line 60 to Col 53 line 25).

*Rabin creates a PKI certificate specifically with unique software call-up policy for each unique Hardware ID. It is clearly that the gaming system must be authorized to run by its associated separate software restriction policy. (Col 28 lines 30-65).*

**8. As per claim 23:**

Rabin discloses “A method according to claim 22, wherein the authorized software components are mandated by a regulatory body” in (Col 47 line 56 to Col 48 line 33).

**9. As per claims 71-72:**

Rabin discloses "A method for a network connected gaming system to prevent unauthorized executable files of constituent computers of the gaming system from executing, comprising the steps of:

packaging the authorized executable files into a code signed installation package;

configuring certificate rule policies to enable execution of the code signed installation package" in (Col 26 lines 50-60, Col 27 lines 30-44, Col 28 lines 5-15, Col 28, Table 1, line 30 to Col 30 line 20, and Col 52 line 60 to Col 53 line 25);

"enforcing the policies, and executing the code signed installation package upon every startup of any of the constituent computers (Col 39 line 60 to Col 40 line 15) of the gaming system or upon a command, wherein execution of any authorized executable file is predicated upon successfully executing the code signed installation package into which the authorized executable file is packaged" in (Col 47 line 56 to Col 48 line 33, and Col 52 line 60 to Col 53 line 25)

**10. As per claims 73-74:**

Rabin discloses "A method for a network connected gaming system to prevent unauthorized executable code of constituent computers of the gaming system from executing, comprising the steps of:

packaging the authorized executable files into a code signed installation package;

Art Unit: 2135

configuring certificate rule policies to enable execution of the code signed installation package” in (Col 26 lines 50-60, Col 27 lines 30-44, Col 28 lines 5-15, Col 28, Table 1, line 30 to Col 30 line 20, and Col 52 line 60 to Col 53 line 25);

“configuring enforcement of the policies, and re-installing the code signed installation package at every computer startup (Col 39 line 60 to Col 40 line 15) of any of the constituent computers of the gaming system or upon a command, wherein execution of any authorized executable file is predicated upon successfully executing the code signed Installation package Into which the authorized executable file is packaged” in (Col 47 line 56 to Col 48 line 33, and Col 52 line 60 to Col 53 line 25).

**11. As per claims 75-78:**

Rabin discloses “A method for a network connected gaming system to prevent data of unauthorized non-executable files code of constituent computers of the gaming system from affecting game outcome, comprising the steps of:

packaging the non-executable files into a code signed installation package” in (Col 26 lines 50-60, Col 27 lines 30-44, Col 28 lines 5-15, Col 28, Table 1, line 30 to Col 30 line 20, and Col 52 line 60 to Col 53 line 25);

“configuring certificate rule policies to enable execution of the code signed installation package;

configuring enforcement of the policies, and

executing the code signed installation package upon every computer startup of any of the constituent computers of the gaming system or upon a command” in (Col 47 line 56 to Col 48 line 33, and Col 52 line 60 to Col 53 line 25).

**12. As per claims 79, and 97:**

Rabin discloses “A method for scheduling at least one authorized executable software component installed in a network connected gaming system, the gaming system including a Plurality of gaming machines, the method comprising the steps of:

packaging at least one authorized non-executable file that control the scheduling of the at least one authorized executable software component into at least one code signed installation package, each of the at least one code signed installation packages a predetermined PKI certificate” in (Col 26 lines 50-60, Col 27 lines 30-44, Col 28 lines 5-15, Col 28, Table 1, line 30 to Col 30 line 20, and Col 52 line 60 to Col 53 line 25);

“configuring certificate rule policies to enable execution of the at least one code signed installation package in selected ones of the plurality of gaming machines; and

configuring enforcement of the certificate rule policies;

and downloading the at least one code signed installation package into is the selected ones of the plurality of earning machines; executing the at least one code signed installation package” in (Col 47 line 56 to Col 48 line 33, and Col 52 line 60 to Col 53 line 25)..

**13. As per claim 81:**

Rabin discloses “A method for scheduling at least one authorized executable software component according to claim 79, further comprising the step of reinstalling the at least one code signed installation package at every startup of any of the constituent gaming machines of the gaming system or upon a command” in (Col 39 line 60 to Col 40 line 15).



Art Unit: 2135

**14. As per claim 94:**

Rabin discloses "A method for a gaming term machine in a network connected gaming system to generate a list menu of authorized games available to players the method comprising the steps of:

generating a separate and unique code signed certificate for a predetermined software module of each authorized game;

generating an executable companion file for each authorized game, wherein the executable companion file is configured to execute faster than the authorized game;

code signing both the predetermined software module and its executable companion file with the generated PKI certificate" in (Col 26 lines 50-60, Col 27 lines 30-44, Col 28 lines 5-15, Col 28, Table 1, line 30 to Col 30 line 20, and Col 52 line 60 to Col 53 line 25);

"enforcing software restriction policy rules for preventing unauthorized software components from executing; enforcing software restriction policy rules for enabling execution of selected ones of the authorized games;

attempting to execute each executable companion File; and

adding only those games to the menu of authorized games whose executable companion file has not been denied execution by the software restriction policy rules" in (Col 47 line 56 to Col 48 line 33, and Col 52 line 60 to Col 53 line 25).

Art Unit: 2135

**15. As per claims 95-96:**

Rabin discloses "A method according to claim 94 further comprising the step of removing games from the menu of authorized games whose companion file is denied execution by the software restriction policy rules" in (Col 40 line 45 to Col 41 line 18).

***Claim Rejections - 35 USC § 103***

**16. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:**

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**17. Claims 1-19, 24-25, and 82-90 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rabin et al, US Patent No. 6697948B1, hereinafter "Rabin", in view of Hall et al, US Patent No. 5920,861, hereinafter "Hall"**

**18. As per claim 1:**

Rabin discloses "A PKI certificate architecture for network connected gaming system, the gaming system including a plurality of gaming machines each having a plurality of executable software components, wherein each different executable software component within each gaming machine within the gaming system (Col 27 lines 1-14, Col 39 lines 20-35, and Col 46 lines 56-62) subject to receive certification is

Art Unit: 2135

uniquely associated with a unique identifier (Table 1, ID(X), ID(SP), and Col 36 lines 30-45) and

is signed with a separate and unique PKI certificate, the separate and unique PKI certificate being uniquely identified at least by the unique identifier" in (Col 28, Table 1, line 30 to Col 30 line 20), and wherein identical executable software components in different ones of the plurality of gaming machines of the network connected gaming system are associated with identical identifiers and are signed with identical PKI certificates

However, Rabin's invention has overcome the problem executing the software by having only cryptographic certificate key. Rabin further utilize the hardware identification, which only allow the software to be executable in a computer device in allowed HW ID. The feature causes to bring about different separate and unique identifier in each PKI certificate, and not having identical PKI certificates.

Nevertheless, Hall on the other hand discloses a method of limiting the executable software in an allowed target environment, such as application program, operating system or combination of both (Col 20 lines 5-24). The target environment parser would collect the data block corresponding to the target environment and cryptographically hashes it to create a unique identification cryptographic key certificate. (Col 19 lines 30-56).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Rabin's invention to incorporate Hall's teaching of using the ID of the target environment to restrict the execution of the

Art Unit: 2135

software. It is obvious that the plurality gaming machines with identical application program or operating system would have identical identification cryptographic key certificate.

**19. As per claim 2:**

Rabin discloses "A PKI certificate architecture according to claim 1, wherein the each software component is authorized by a regulatory authority" in (Col 32 lines 5-25, and Table 1, Col 28 line 30 to Col 30 line 20).

**20. As per claim 3:**

Rabin discloses "A PKI certificate architecture according to claim 1, wherein the distinctive separate and unique PKI certificate is produced by the certification lab, by the gaming system supplier or by the trusted party designated by the regulatory authority" in (Col 32 lines 5-25, and Table 1, Col 28 line 30 to Col 30 line 20).

**21. As per claim 4:**

Rabin discloses "A PKI certificate architecture according to claim 1, wherein each software component is code signed by the a certification lab, by the gaming system supplier or by the a misted party designated by the regulatory authority" in (Col 32 lines 5-25, and Table 1, Col 28 line 30 to Col 30 line 20).

**22. As per claim 5:**

Rabin discloses "A PKI certificate architecture according to claim 1, wherein the separate and unique identifier is a certificate field selected from a "Subject" field, an "issued to" field, a "subject name" field, the a "CommonName" field, a "Provider" field or a "publisher" field" in (Col 32 lines 5-25, and Table 1, Col 28 line 30 to Col 30 line 20).

**23. As per claim 6:**

Rabin discloses "A PKI certificate architecture according to claim 1, wherein the unique identifier comprises at least one of fields and field extensions" in (Col 32 lines 5-25, and Table 1, Col 28 line 30 to Col 30 line 20).

**24. As per claim 7:**

Rabin discloses "A PKI certificate architecture according to claim 1, wherein the unique Identifier comprises at least one of a plurality of fields selected from among: a software component part number; a software component major version number; a software component minor version number; a software component build number; a software component revision number; a software component project name; a software component type of software component; a software component language variant; a software component game regulation variant; a software component friendly name; an identification of the certification laboratory, and an identification of the client" in (Col 32 lines 5-25, and Table 1, Col 28 line 30 to Col 30 line 20).

**25. As per claim 8:**

Rabin discloses "A PKI certificate architecture according to claim 7, wherein the unique identifier is a concatenation of selected Identifiers fields" in (Col 32 lines 5-25, and Table 1, Col 28 line 30 to Col 30 line 20).

**26. As per claim 9:**

Rabin discloses "A PKI certificate architecture according to claim 1, wherein at least a portion of the unique identifier is reported in the Windows event log upon execution of the software component" in (Col 59 lines 1-28).

**27. As per claim 10:**

Rabin discloses "A PKI certificate architecture according to claim 1, wherein at least a portion of the unique identifier is reported in the source held of the Windows event log upon execution of the software component" in (Col 59 lines 1-28).

**28. As per claim 11:**

Rabin discloses "A PKI certificate architecture according to claim 1, wherein at least a portion of the unique identifier is reported in the Windows event log upon execution of

the software component in a predetermined event log bin upon execution of the software component” in (Col 59 lines 1-28).

**29. As per claim 12:**

Rabin discloses “A PKI certificate architecture according to claim 1, wherein at least a portion of the unique Identifier is traceable in at least one of: source code; Windows File Properties; Trusted Inventory; Windows Event Log; Software Restriction Policies, and Certificate Store” in (Col 59 lines 1-28).

**30. As per claim 13-14:**

Rabin discloses “A PKI certificate architecture according to claim 1, wherein the network connected gaming system is connected in at least one of a local area system and wide area network” in (Col 27 lines 1-14).

**31. As per claim 15:**

Rabin discloses “A PKI certificate architecture according to claim 1, wherein the unique identifier contains identification information delimited with file-name-allowed non-alphanumeric characters to facilitate human identification, string searches and file searches” in (Col 32 lines 5-25, and Table 1, Col 28 line 30 to Col 30 line 20).

**32. As per claim 16:**

Rabin discloses "A PKI certificate architecture according to claim 1, wherein a selected set of identification information making up the identifier are used for making up the file name of PKI certificate related files such as \*.CER, \*.P7B and \*.PVK such as to facilitate human identification, string searches and file searches" in (Col 7 lines 55-65).

**33. As per claim 17:**

Rabin discloses "A method for a network connected gaming system to prevent unauthorized software components of constituent computers of the gaming system from executing (Col 27 lines 1-14, Col 39 lines 20-35, and Col 46 lines 56-62) the gaming system including a plurality of gaming machines each having a plurality of executable software components, the method comprising "the steps of:

producing a separate and unique PKI certificate for each of the plurality of executable software component subject to receiving certification within each gaming machine, each software component subject to receiving certification including a unique identifier;

code signing each executable software component subject to receiving certification with its respective separate and unique PKI certificate, each respective PKI certificate being uniquely identified at least by a unique identifier that is uniquely associated with the executable software component such that identical executable software components in different ones of the plurality of gaming machines of the network connected gaming system are associated with identical identifiers and are code signed with identical PKI



Art Unit: 2135

certificates, and configuring software restriction policy certificate rules to allow execution of only those executable software components whose code signed PKI certificate is determined to be authorized" in (Col 26 lines 50-60, Col 27 lines 30-44, Col 28 lines 5-15, Col 28, Table 1, line 30 to Col 30 line 20, and Col 52 line 60 to Col 53 line 25).

However, Rabin's invention has overcome the problem executing the software by having only cryptographic certificate key. Rabin further utilize the hardware identification, which only allow the software to be executable in a computer device in allowed HW ID. The feature causes to bring about different separate and unique identifier in each PKI certificate, and not having identical PKI certificates.

Nevertheless, Hall on the other hand discloses a method of limiting the executable software in an allowed target environment, such as application program, operating system or combination of both (Col 20 lines 5-24). The target environment parser would collect the data block corresponding to the target environment and cryptographically hashes it to create a unique identification cryptographic key certificate. (Col 19 lines 30-56).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Rabin's invention to incorporate Hall's teaching of using the ID of the target environment to restrict the execution of the software. It is obvious that the plurality gaming machines with identical application program or operating system would have identical identification cryptographic key certificate.

**34. As per claim 18:**

Rabin discloses "A method according to claim 17, further comprising the step of configuring Software restriction policy rules to prevent execution of unauthorized software components" in (Col 26 lines 50-60, Col 27 lines 30-44, Col 28 lines 5-15, Col 28, Table 1, line 30 to Col 30 line 20, and Col 52 line 60 to Col 53 line 25)..

**35. As per claim 19:**

Rabin discloses "A method according to claim 17, further comprising the step of configuring software restriction policy rules to prevent execution of all not explicitly authorized software components" in (Col 26 lines 50-60, Col 27 lines 30-44, Col 28 lines 5-15, Col 28, Table 1, line 30 to Col 30 line 20, and Col 52 line 60 to Col 53 line 25).

**36. As per claim 24:**

Rabin discloses "A method for a network connected gaming system, to enable only authorized software components of constituent computers of the gaming system to execute, the gaming system including a plurality of gaming machines each having a plurality of executable software components, the method comprising the steps of producing a separate and unique PKI certificate for each of the plurality of executable software component within the gaming system subject to receive certification, each respective PKI certificate being associated with a unique identifier that is uniquely associated with the software component such that identical executable software components in different ones of the plurality of gaming machines of the

Art Unit: 2135

network connected gaming system are associated with identical identifiers and are code signed with identical PKI certificates;

signing each software component subject to receive certification with the its respective separate and unique PKI certificate" in (Col 26 lines 50-60, Col 27 lines 30-44, Col 28 lines 5-15, Col 28, Table 1, line 30 to Col 30 line 20, and Col 52 line 60 to Col 53 line 25);

"configuring a certificate software restriction policy for each of the respective separate and unique PKI certificates, and

enforcing, the certificate software restriction policy for each of the respective separate and unique PKI certificates" in (Col 47 line 56 to Col 48 line 33, and Col 52 line 60 to Col 53 line 25).

*Rabin creates a PKI certificate specifically with unique software call-up policy for each unique Hardware ID. It is clearly that the gaming system must be authorized to run by its associated separate software restriction policy. (Col 28 lines 30-65).*

However, Rabin's invention has overcome the problem executing the software by having only cryptographic certificate key. Rabin further utilize the hardware identification, which only allow the software to be executable in a computer device in allowed HW ID. The feature causes to bring about different separate and unique identifier in each PKI certificate, and not having identical PKI certificates.

Nevertheless, Hall on the other hand discloses a method of limiting the executable software in an allowed target environment, such as application program, operating system or combination of both (Col 20 lines 5-24). The target environment

Art Unit: 2135

parser would collect the data block corresponding to the target environment and cryptographically hashes it to create a unique identification cryptographic key certificate. (Col 19 lines 30-56).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Rabin's invention to incorporate Hall's teaching of using the ID of the target environment to restrict the execution of the software. It is obvious that the plurality gaming machines with identical application program or operating system would have identical identification cryptographic key certificate.

**37. As per claim 25:**

Rabin discloses "A method for downloading authorized software components and allowing execution of downloaded authorized executable software components of a of a plurality of gaming machines of a network connected gaming system, comprising the steps of

For each of the plurality of gaming machines of the network connected gaming system:

code signing each authorized executable software component with a separate PKI certificate that is unique to the authorized software component such that identical executable software components in different ones of the plurality of gaming machines of the network connected gaming system are code signed with identical PKI certificates."

Art Unit: 2135

in (Col 26 lines 50-60, Col 27 lines 30-44, Col 28 lines 5-15, Col 28, Table 1, line 30 to Col 30 line 20, and Col 52 line 60 to Col 53 line 25);

“Packaging the code signed authorized executable software components into an installation package; configuring install policies to install each code signed authorized software component contained in the installation package;

configuring certificate rule policies to allow execution of the installed code signed authorized executable software component; and

configuring enforcement of the policies” in (Col 47 line 56 to Col 48 line 33, and Col 52 line 60 to Col 53 line 25).

*Rabin creates a PKI certificate specifically with unique software call-up policy for each unique Hardware ID. It is clearly that the gaming system must be authorized to run by its associated separate software restriction policy. (Col 28 lines 30-65).*

However, Rabin’s invention has overcome the problem executing the software by having only cryptographic certificate key. Rabin further utilize the hardware identification, which only allow the software to be executable in a computer device in allowed HW ID. The feature causes to bring about different separate and unique identifier in each PKI certificate, and not having identical PKI certificates.

Nevertheless, Hall on the other hand discloses a method of limiting the executable software in an allowed target environment, such as application program, operating system or combination of both (Col 20 lines 5-24). The target environment parser would collect the data block corresponding to the target environment and

Art Unit: 2135

cryptographically hashes it to create a unique identification cryptographic key certificate.  
(Col 19 lines 30-56).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Rabin's invention to incorporate Hall's teaching of using the ID of the target environment to restrict the execution of the software. It is obvious that the plurality gaming machines with identical application program or operating system would have identical identification cryptographic key certificate.

**38. As per claim 82:**

An automate platform to enable an on-going regulatory certificateion of a plurality of authorized software components of a network connected gaming system including a plurality of computers, the method comprising:

A reference platform representative of a target network connected gaming system and comprising a software-building environment located at a manufacturer or subcontractor of the software components;

A certification platform located at a regulatory certification authority, the certification platform bing substantially identical to the reference platform, and

Code-signing means for enabling the manufacturer or subcontractor to associate a separate and unique PKI certificate with each authorized software component subject to regulatory certification such identical authorized software components subject to

regulatory certification in different ones of the plurality of gaming machines of the network connected gaming system are code signed with identical PKI certificates.

However, Rabin's invention has overcome the problem executing the software by having only cryptographic certificate key. Rabin further utilize the hardware identification, which only allow the software to be executable in a computer device in allowed HW ID. The feature causes to bring about different separate and unique identifier in each PKI certificate, and not having identical PKI certificates.

Nevertheless, Hall on the other hand discloses a method of limiting the executable software in an allowed target environment, such as application program, operating system or combination of both (Col 20 lines 5-24). The target environment parser would collect the data block corresponding to the target environment and cryptographically hashes it to create a unique identification cryptographic key certificate. (Col 19 lines 30-56).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Rabin's invention to incorporate Hall's teaching of using the ID of the target environment to restrict the execution of the software. It is obvious that the plurality gaming machines with identical application program or operating system would have identical identification cryptographic key certificate.

Art Unit: 2135

**39. As per claims 83 and 86-89:**

Rabin discloses "An automated platform according to claim, 82, further comprising a secure communication link between the reference platform and the certification lap for enabling manufacturer or designated subcontractors to remotely configure the software building environment on tile certification platform" in (Col 27 lines 30-65).

**40. As per claims 84-85 and 90:**

Rabin discloses "An automated platform according to claim 82, wherein the authorized software components to be downloaded to the network connected gaming system is are tested by the certification laboratory" in (Col 27 lines 30-44).

**41. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).**


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.



Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son  
Examiner  
Art Unit 2135

  
AU 2135